

Guardian Week 1: Lock It Down

Mon, Dec 7 – Tue, Dec 8 · 2:30–4:00 PM · Room 105 (or live on Zoom; the link comes by email)

This week: Build passwords that hold up, add a second factor, and learn the security ideas behind every defense. Tuesday is capture-the-flag.

Heads up

- Never use a real password in class activities. Everything this week uses made-up practice passwords.

Read-aheads

Before Monday (15 minutes)

- Read the Passwords and logins notes below.
- Check one of your own accounts: is multifactor authentication on? (Don't share the answer or any password with anyone.)
- Play one round of Password Lab in the Arcade.

Before Tuesday (15 minutes)

- Read the Security ideas and Encryption notes below.
- Do 15 Guardian study cards.
- Try the Check yourself questions.

The missions

Monday, Dec 7 · Day 17

10A · Game Crack-Proof

How long would it take to crack your password? Your crew rates a set of made-up passwords, learns why length beats complexity, and sets up a password manager and multifactor authentication on a practice account. Then you learn the CIA triad that every security choice protects.

1. Play Password Lab and rate all 12 passwords, then explain the three biggest mistakes you saw.
2. Set up a practice password-manager vault and enable MFA with an authenticator app.
3. Match five security scenarios to confidentiality, integrity, or availability.

Turn in: Password Lab score, MFA setup screenshot, and the CIA matching sheet.

Tuesday, Dec 8 · Day 18

Mr. James sets up picoCTF access in class. Please don't make an account at home first.

10B · Game picoGym Crew Hunt

Capture-the-flag time. Your crew tackles beginner picoGym challenges that teach encryption, encoding, and careful reading of clues. Each solved challenge reveals a flag, and each flag connects back to a Tech+ security idea like encryption at rest and in transit.

1. Create crew accounts on picoCTF and solve at least three beginner General Skills or Cryptography challenges.
2. For each flag, write one sentence connecting the challenge to a Tech+ security concept.
3. Share one solving tip with another crew.

Turn in: List of solved challenges with flags redacted and the three concept connections.

Notes

Passwords and logins

- Length beats complexity. A long passphrase of random words (orbit-marble-lantern-fox-71) is stronger than a short jumble.
- Never reuse a password. One breach then unlocks every account that shares it.
- A password manager creates and remembers a strong, unique password for every site. You remember one master password.
- Authentication factors: something you know (password, PIN), something you have (phone, security key), something you are (fingerprint, face).
- Multifactor authentication (MFA) combines two different factor types, like a password plus a code from an authenticator app.

Security ideas

- CIA triad: Confidentiality (only the right people can see it), Integrity (it hasn't been changed), Availability (it works when people need it).
- AAA: Authentication (who are you?), Authorization (what are you allowed to do?), Accounting (a log of what you did).
- Least privilege: give each person only the access their job needs.

Encryption and encoding

- Encryption scrambles data so only someone with the key can read it.
- At rest: data stored on a device (full-disk encryption protects a stolen laptop).
- In transit: data moving across a network (HTTPS and VPNs).
- A hash is a fingerprint of a file. If the hash changes, the file changed (integrity).
- Encoding (like Base64) only changes the format. Anyone can reverse it, so it is not security.

Vocabulary

MFA	Multifactor authentication: two or more factor types
Passphrase	A long password made of several words
CIA triad	Confidentiality, Integrity, Availability
Least privilege	Only the access you need
Encryption	Scrambling data so only key holders can read it
Hash	A fixed fingerprint of data used to detect changes

Check yourself

1. A fingerprint scan is which factor?
2. A server is flooded so nobody can log in. Which part of the CIA triad is hit?
3. Is Base64 a way to keep a secret?

Answers: 1. Something you are 2. Availability 3. No. It's encoding, and anyone can decode it.

Bring

- A charged device
- Your student ID card
- Headphones (optional)